UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/681,203	02/21/2001	Ariel Katz	1018.126US1	5124

23460 7590 05/04/2005

LEYDIG VOIT & MAYER, LTD
TWO PRUDENTIAL PLAZA, SUITE 4900
180 NORTH STETSON AVENUE
CHICAGO, IL 60601-6780

EXAMINER	
LAFORGIA, CHRISTIAN A	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 05/04/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/681,203	KATZ ET AL.	
	Examiner	Art Unit	
	Christian La Forgia	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 December 2004*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *23 December 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. The amendment filed on 23 December 2004 has been noted and made of record.

2. Claims 1-36 have been presented for examination.

Drawings

3. The drawings were received on 23 December 2004. The Examiner accepts these drawings.

Response to Arguments

4. Applicant's arguments filed 23 December 2004 have been fully considered but they are not persuasive.

5. The Examiner is not persuaded by the Applicant's arguments that the Examiner's interpretation is inappropriate because is attributes features or limitations not recited in the claim limitations. The Applicant is reminded that office personnel are to give the claims their broadest reasonable interpretation in light of the specification. See MPEP § 904.01. See MPEP § 2111- § 2116.01. See *In re Morris*, 127 F.3d 1048, 44 USPQ2d 1023 (Fed. Cir. 1997). Page 3, paragraph [0007] of the specification reads as:

> The proxy decrypts the encrypted data, and performs an action, or test, relative to the data, such as ensuring that the data does not present a security risk, and offering the benefit of redirecting the traffic as appropriate.

Therefore, the Examiner's interpretation of the claim language is appropriate and the rejection proper.

6. In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge

generally available to one of ordinary skill in the art. See *In re Fine*, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and *In re Jones*, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, both references offer reasons/motivation for the combination of the references as cited below.

7. As per the Applicant's argument that Ranger never discloses that the data is transmitted either to an intended receipt or an origin server, the Examiner respectfully disagrees. Ranger discloses at column 2, lines 43-46 that:

> This [virus detection] may be done prior to allocating use of the decrypted digital information by other computers or prior to transferring data to other computers or other applications within a computer.

Ranger further goes on to state in column 2, lines 51-56 that:

> For example, the system decrypts the detected encrypted digital input information and applies virus detection to the decrypted digital information in response to the virus detection request, prior to allowing use or transfer of the decrypted digital input information.

Therefore, Ranger discloses transmitting data and the rejection is proper.

8. See further rejections that follow.

Claim Rejections - 35 USC § 103

9. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

10. Claims 1-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,681,327 to Jardin, hereinafter Jardin, in view of U.S. Patent No. 6,393,568 to Ranger et al., hereinafter Ranger.

11. As per claim 1, Jardin teaches a method comprising:

receiving encrypted data from a client over an unsecure network in a first hop (Figures 1 [blocks 150], 3 [block 310], column 6, lines 1-13);

decrypting the encrypted data into decrypted data (Figure 3 [block 330], column 6, line 58 to column 7, line 5).

12. Jardin does not disclose performing a test relative to the decrypted data, the test yielding one of at least a first result and a second result.

13. Ranger discloses performing a test relative to the decrypted data, the test yielding one of at least a first result and a second result, wherein the Examiner interprets the first result as the data not presenting a security risk and the second result as the data presenting a security risk. It would have been obvious to one of ordinary skill in the art at the time the invention was made to test the data for malicious code, since Ranger discloses at column 2, line 64 to column 3, line 15 that such a modification would prevent malicious code from being executed on a computer or transferred to other computers or applications within a network. Subsequently if the data did not contain a virus, Trojan horse, or any other malicious code, the decrypted data would be transferred to a server over a given network in the second hop. Jardin discloses transmitting the data to a server in at least figure 3, blocks 336 and 346, and column 7, lines 10-15 and lines 53-56. Ranger discloses transmitting uninfected data to the intended recipient after it has been determined that it does not contain malicious code in column 4, lines 38-53.

14. Regarding claims 2 and 15, Ranger teaches wherein performing the test relative to the decrypted data comprises examining the decrypted data for security purposes, such that the first result is the decrypted data not presenting the security risk (column 2, lines 24-56).

15. Regarding claim 3, Jardin teaches wherein sending the decrypted data to the origin server over the given network in the second hop comprises first encrypting the decrypted data into second encrypted data (Figure 3 [blocks 336]; column 7, lines 6-19).

16. Regarding claim 4, Jardin teaches wherein the given network is a secure network (column 6, lines 44-57).

17. With regards to claims 5 and 16, Jardin discloses wherein the servers are web servers thereby able to handle HTTP and IMAP.

18. Ranger discloses scanning e-mails thereby accounting for POP.

19. Regarding claim 6, neither Jardin nor Ranger teaches wherein the given network is one of the unsecure network and a second unsecure network. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the network comprise of a first and second network, since it has been held that merely rearranging the orientation of computers into a hierarchical fashion is a design choice typically made by the network engineer. See MPEP 2144.04; see *In re Japikse*, 181 F.2d 1019, 1023, 86 USPQ 70, 73 (CCPA 1950).

20. Regarding claim 7, Jardin teaches wherein the encrypted data is received from the client over the unsecure network in the first hop within a secure socket layer (SSL) session (column 4, lines 24-34).

21. Regarding claims 8 and 19, Jardin teaches wherein the unsecure network is the Internet (Figure 1 [block 150]; column 3, lines 46-60).

22. Regarding claims 9 and 24, Jardin teaches wherein the origin server is an effective origin server (column 3, line 61-67).

23. Regarding claims 10 and 23, Jardin teaches wherein the client is an effective client (column 3, lines 46-60).

24. Regarding claims 11 and 25, Ranger teaches wherein the method is performed by a proxy within the given network (Figure 4 [block 64]; column 4, lines 34-47; column 5, lines 41-58).

25. Regarding claims 12 and 26, Ranger teaches wherein the method is performed by a firewall within the given network (Figure 4 [block 64]; column 3, line 66 to column 4, line 21; column 5, lines 41-58).

26. Regarding claims 13 and 27, Ranger teaches a computer-readable medium having a computer program stored thereon for execution by a processor (column 3, lines 41-46).

27. As per claim 14, Jardin teaches a method comprising:

receiving unencrypted data from a client over a secure network in a first hop (column 4, lines 34-43);

28. Jardin does not disclose performing a test relative to the unencrypted data, the test yielding one of at least a first result and a second result.

29. Ranger discloses performing a test relative to the unencrypted data, the test yielding one of at least a first result and a second result, wherein the Examiner interprets the first result as the data not presenting a security risk and the second result as the data presenting a security risk. It would have been obvious to one of ordinary skill in the art at the time the invention was made to test the data for malicious code, since Ranger discloses at column 2, line 64 to column 3, line 15 that such a modification would prevent malicious code from being executed on a computer or transferred to other computers or applications within a network. Subsequently if the data did not contain a virus, Trojan horse, or any other malicious code, the unencrypted data would be transferred to a server over a given network in the second hop.

30. Jardin discloses encrypting the unencrypted data into encrypted data (Figure 3 [blocks 336]; column 7, lines 6-19).

31. Both Jardin and Ranger disclose transmitting the encrypted data to a server over an unsecure network. Jardin discuses this in at least figure 3, blocks 336 and 346, as well as column 7, lines 10-15 and lines 53-56, while Ranger offers discussion of this in at least column 4, lines 35-53.

32. Regarding claim 17, Jardin teaches wherein the encrypted data is sent to the origin server over the unsecure network in the second hop within a secure socket layer (SSL) session (column 7, lines 6-19).

33. Regarding claim 18, Ranger teaches wherein the secure network is a carrier network (Figure 4; column 5, line 41 to column 6, line 18).

34. Regarding claim 20, Jardin teaches wherein the client is a thin client (Figure 1 [block 110]; column 3, lines 46-60).

35. Regarding claim 21, Jardin teaches wherein the client is one of a: personal digital assistant (PDA) device, a laptop computer, a notebook computer, and a wireless phone (Figure 1 [block 110]; column 3, lines 46-60).

36. Regarding claim 22, Jardin teaches wherein the secure network is one of a wired network (Figure 1, column 3, lines 46-60).

37. Jardin and Ranger do not disclose the use of a secure wireless network

38. It would have been obvious to one of ordinary skill in the art at the time the invention was made to include a secure wireless network, since it has been held that it requires only ordinary skill in the art to enable a network to be portable and remove wires to make the network more aesthetically pleasant. See MPEP § 2144.04; see *In re Seid*, 161 F.2d 229, 231, 73 USPQ 431, 433 (CCPA 1947); see *In re Lindberg*, 194 F.2d 732, 735, 93 USPQ 23, 26 (CCPA 1952).

39. As per claim 28, Jardin teaches a system comprising:

a client to send encrypted data over an unsecure network in a first hop (Figures 1 [blocks 110, 150], 3 [blocks 310]; column 6, lines 1-13);

a proxy within a secure network to receive the encrypted data and decrypt the encrypted data into decrypted data, the proxy sending the decrypted data over the secure network in a second hop (Figures 1 [block 120], 3 [blocks 330, 340]; column 4, lines 34-47; column 6, line 58 to column 7, line 5; column 7, lines 38-57); and,

an origin server within the secure network to receive the decrypted data (Figure 3 [block 346]; column 7, lines 38-57).

40. Jardin does not disclose wherein the data is transmitted in response to performing a test relative to the decrypted data yielding a particular response.

41. Ranger discusses wherein the data is transmitted in response to performing a test relative to the decrypted data yielding a particular response, wherein the Examiner interprets the response to be the virus free result of a virus check performed on the data. It would have been obvious to one of ordinary skill in the art at the time the invention was made to test the data for malicious code, since Ranger discloses at column 2, line 64 to column 3, line 15 that such a modification would prevent malicious code from being executed on a computer or transferred to other computers or applications within a network.

42. Regarding claim 29, Jardin discloses sending unencrypted data over a secure network in column 4, lines 24-47. Jardin also discloses a proxy within a secure network to receive the unencrypted data, wherein the second proxy encrypts the unencrypted data into encrypted data and sending the encrypted data over an unsecure network in at least figure 3, blocks 336 and 346, as well as column 7, lines 10-15 and lines 53-56.

43. It would have been obvious to one of ordinary skill in the art to include a second client and second proxy, since it has been held that duplicating a part to have a multiple effect requires only ordinary skill in the art. See MPEP 2144.04; see *In re Harza*, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960). This is particularly important if the test yields a second result, which the Examiner interprets as the data having malicious code, because it would allow the malicious code to be quarantined thereby making it unable to infect other computers or applications.

44. Regarding claim 30, Jardin discloses a client to send encrypted data over an unsecure network in at least Figures 1 [blocks 150], 3 [block 310], column 6, lines 1-13. Jardin also discusses the use of a proxy to receive encrypted data, decrypt the encrypted data, and transmitting the encrypted data over the unsecure network.

45. It would have been obvious to one of ordinary skill in the art to include a second client and second proxy, since it has been held that duplicating a part to have a multiple effect requires only ordinary skill in the art. See MPEP 2144.04; see *In re Harza*, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960). This is particularly important if the test yields a second result, which the Examiner interprets as the data having malicious code, because it would allow the malicious code to be quarantined thereby making it unable to infect other computers or applications.

46. As per claim 31, Jardin teaches a system comprising:

a client to send unencrypted data over a secure network in a first hop (column 4, lines 34-43);

a proxy within the secure network to receive the unencrypted data, the proxy encrypting the unencrypted data into encrypted data and sending the encrypted data over an unsecure network in a second hop (Figures 1 [block 120], 3 [blocks 330, 336, 340]; column 4, lines 34-47; column 6, line 58 to column 7, line 19); and,

an origin server to receive the encrypted data (Figure 3, blocks 336 and 346, as well as column 7, lines 10-15 and lines 53-56).

47. Jardin does not disclose wherein the data is transmitted in response to performing a test relative to the unencrypted data yielding a particular response.

48. Ranger discusses wherein the data is transmitted in response to performing a test relative to the unencrypted data yielding a particular response, wherein the Examiner interprets the response to be the virus free result of a virus check performed on the data. It would have been obvious to one of ordinary skill in the art at the time the invention was made to test the data for malicious code, since Ranger discloses at column 2, line 64 to column 3, line 15 that such a modification would prevent malicious code from being executed on a computer or transferred to other computers or applications within a network.

49. Regarding claim 32, Jardin discloses a proxy within a secure network to receive encrypted data encrypted data and decrypt the encrypted data into decrypted data and sending the decrypted data over the secure network to be received by a server in at least figures 1, block 120, 3, blocks 340 and 346, as well as column 4, lines 34-47 and column 7, lines 38-57.

50. It would have been obvious to one of ordinary skill in the art to include a second proxy and a second server, since it has been held that duplicating a part to have a multiple effect requires only ordinary skill in the art. See MPEP 2144.04; see *In re Harza*, 274 F.2d 669, 671, 124 USPQ 378, 380 (CCPA 1960).

51. As per claim 33, Jardin teaches a proxy comprising:

one or more communication components enabling the proxy to communicate over a first network and a second network (Figure 1 [blocks 118, 128]; column 3, lines 46-60);

a computer-readable medium having a computer program stored thereon for execution by the processor to receive data that is originally encrypted or unencrypted from a client over the first network in a first hop and decrypt the data where the data was originally encrypted, sending the data unencrypted to an origin server over the second network in a second hop where the data was originally encrypted, and sending the data unencrypted or encrypted to the origin server over the second network in a second hop where the data was originally unencrypted (Figures 1 [blocks 150], 3 [blocks 310, 330, 336, 346], column 4, lines 34-43; column 6, lines 1-13, column 6, line 58 to column 7, line 19; column 7, lines 53-56). Typical Internet devices described in Jardin comprise processors.

52. Jardin does not disclose performing a test relative to the decrypted data, the test yielding one of at least a first result and a second result.

53. Ranger discloses performing a test relative to the decrypted data, the test yielding one of at least a first result and a second result, wherein the Examiner interprets the first result as the data not presenting a security risk and the second result as the data presenting a security risk. It would have been obvious to one of ordinary skill in the art at the time the invention was made to test the data for malicious code, since Ranger discloses at column 2, line 64 to column 3, line 15 that such a modification would prevent malicious code from being executed on a computer or transferred to other computers or applications within a network.

54. Regarding claim 34, Jardin teaches wherein the first network is a secure network (column 4, lines 24-47).

55. Regarding claim 35, Jardin teaches wherein the second network is an unsecure network, such that sending the data to the origin server over the second network in the second hop comprises first encrypting the data (Figure 3 [block 336, 338]; column 7, liens 6-38).

56. Regarding claim 36, Jardin teaches wherein the second network is a secure network (column 7, lines 6-19).

Conclusion

57. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

58. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

59. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christian La Forgia whose telephone number is (571) 272-3792. The examiner can normally be reached on Monday thru Thursday 7-5.

60. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

61. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christian LaForgia
Patent Examiner
Art Unit 2131
clf

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100